UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/456,794 | 12/08/1999 | JAY C. CHEN | 34581/CAG/C718 | 6924 |

7590 07/02/2002

CHRISTIE PARKER & HALE LLP
PO BOX 7068
PASADENA, CA 911097068

| EXAMINER |
|---|
| MEISLAHN, DOUGLAS J |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

DATE MAILED: 07/02/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 00/000,000 | <Unknown> | |
| | Examiner | Art Unit | |
| | Douglas J. Meislahn | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-12* are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *12-8-99* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

***Election/Restrictions***

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-12 are drawn to an electronic card and terminal apparatus, classified in class 713, subclass 185.

   II. Claims 13-53, drawn to a method of key exchange, classified in class 380, subclass 279.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as use in identification systems. See MPEP § 806.05(d).

3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, restriction for examination purposes as indicated is proper.

5. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

6. During a telephone conversation with Craig Gelfound on 19 October 2001 a provisional election was made with traverse to prosecute the invention of group II ,

claims 13-53. Affirmation of this election must be made by applicant in replying to this Office action. Claims 1-12 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

## DETAILED ACTION

### *Drawings*

7. The drawings are objected to because elements 1-10 in figure 2 and 50 and 1180 in figure 12 are not labeled. Correction is required.

### *Claim Objections*

8. Claims 28 and 32 are objected to because of the following informalities: in line 7 of claim 28, "singing" should be "signing"; in line 1 of claim 32, "chooses" should be "choose". Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 24, 28-37, 39, and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claim 24 recites the limitation "his acknowledgement data" and "his acknowledgement message". There is insufficient antecedent basis for this limitation in the claim. Neither the data nor the message have been mentioned, let alone assigned to an entity. These inconsistencies preclude the claim from being examined, although it is surmised that the claim's subject matter is covered by the rejection of claim 23.

12. Claim 28 recites the limitation "the response to member challenge" in line 14 and "the member response" in line 17. There is insufficient antecedent basis for these limitations in the claim.

13. Claim 39 recites the limitation "the first member's session key" in the third line of the claim. There is insufficient antecedent basis for this limitation in the claim. This ambiguity makes the claim and its dependents unexaminable.

***Claim Rejections - 35 USC § 102***

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claim 13 is rejected under 35 U.S.C. 102(b) as being anticipated by Schneier.

On page 47, Schneier presents a method of receiving a session key that includes sending a request (1) (formatting is inherent before sending), generating a session key at a service provider and distributing the key (2), and conducting a transaction (6).

***Claim Rejections - 35 USC § 103***

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 14-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier.

Schneier teaches providing keys in the manner described in claim 14, as has been shown in the discussion of claim 13, but this section does not detail challenges and responses. In the discussion of SKID2 and 3 on pages 55 and 56, Schneier teaches a simple method of authentication that operates on the challenge response principle. In this method, a first entity sends a random number challenge to a second entity, thereby rendering obvious applicant's member challenge. The second entity sends a response to the random number challenge, thereby covering applicant's response for the member challenge. In step 4 of the SKID protocol, the first entity sends a response that is based on response to the random number challenge to the second entity. This method authenticates the two entities to each other. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the SKID3 protocol to authenticate the two entities of Schneier's key exchange method.

With respect to claims 15-17, Schneier has not yet been cited as saying that the transaction is carried out with the service provider. On page 43 Schneier talks about including digital signatures with messages as a means of authenticating the messages to the involved entities and any other parties. Schneier does not mention using the symmetric key to protect information, such as account information, a transaction amount, and sensitive transaction data. Official notice is taken that it is old and well known for a purchaser to encrypt data, including account information, a transaction amount, and sensitive transaction data, with a symmetric key in an electronic transaction in order to prevent that data from being used illicitly. Therefore it would

have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt transaction data sent between the two entities in order to protect data. Data that need not be protected should not be, thereby reducing cryptographic operations and meeting the limitations of claims 17 and 21.

Schneier has not mandated that the entities include transaction identifiers with their transaction correspondences. Official notice is taken that it is old and well known to include transaction identifiers with their transaction correspondences, which helps catalog and identify messages. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include transaction identifiers with their transaction correspondences in order to track messages.

Including the first entity's response to the random number challenge response would minimize traffic. This meets the limitations of claim 19. The rationale behind the rejection of claim 20 is the same.

Official notice is taken that transaction acknowledgement messages are old and well known as clarifying the state of a transaction. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for an encrypted (and hence secure) transaction acknowledgement message to be sent to a service provider.

18. Claims 28-37, 41-44, and 46-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier. The following does not rely on the 102 rejection of claim 13.

The Woo-Lam protocol, as described on page 64 of Schneier, largely covers the

details of claim 28. The first two clauses of the claim are covered by step 3, as is the fifth clause. In step six, Bob generates a challenge, which reads on clause 6. Clause 7 is met by Bob's reception and decryption of the session key. The aforementioned step six also covers clauses 8, 9, and 11. Step 7 covers clauses 12, 13, and 15. The Woo-Lam protocol does not cover the inclusion of Alice's public key as detailed in clause 3 or the signatures in clauses 4, 10, and 14. Including signatures, as mentioned in clauses 4, 10, and 14 is a known method of providing authentication and is displayed on pages 576-577 as part of the ISO authentication framework. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to sign all messages in the Woo-Lam key exchange with authentication protocol as taught in other authentication systems so as to provide another level of authenticity. With regard to the inclusion of Alice's public key, it is included for the convenience of Bob in applicant's embodiment. This provides advantages, such as reduction of the reliance on Trent, but increases forgery risks (see Schneier, page 50). As such, applicant's decision to include the public key with the message would have been apparent to a person of ordinary skill in the art at the time the invention was made.

Regarding claim 29, the EKE protocol described on pages 518 and 519 uses a new public/private key pair with each session. This protects encrypted transmissions from reuse. (It also shows an example of a public key being sent from Alice to Bob). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use different public/private key pairs with each transaction in order to eliminate the possibility of replay attacks.

The rationale behind including plaintext with messages has been discussed before. Encrypting Alice's public key with Bob's public key would be obvious in view of the ISO teaching of encrypting data for security, thereby meeting the limitations of claim 31. Claim 32 is met by the structure of the Woo-Lam protocol. Step 6 of the Woo-Lam protocol renders claim 33 obvious. Transaction identification has been previously discussed. The same rationale meets the limitations of claims 34-37.

The limitations of claim 41 are met if the first member is the only member, a situation that is not precluded by the claim. The same applies to claims 42-44, 46, and 47. Claims 48-53 are met by the teaching on page 50 of the security benefit of receiving signed public keys from a trusted authority.

19. Claims 38 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Thompson et al. (6282552).

Schneier teaches a method for exchanging keys. He does not show the group method of key request. Thompson et al show a method by which changes to a document are recorded. This method entails signing all changes. For the purposes of this discussion, we will assume that Thompson et al.'s original bill corresponds to applicant's key exchange request. As can be seen in figure 5, the original bill has been signed by the originator and then modified and signed by a second entity, whereby the original bill remains perceptible. The benefit of this is that it allows parties to know exactly what different entities added, as taught in lines 29 and 30 of column 5. Therefore it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to include signatures and recognizable updates as taught by Thompson et al. in Schneier's key exchange requests.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail O. Hayes can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
December 18, 2001

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100